

=====

H I P A A n o t e -- Volume 2, Number 29 -- July 31, 2002

>>From Phoenix Health Systems--HIPAA Knowledge--HIPAA Solutions<<  
=>Healthcare IT Consulting & Outsourcing<=

=====

IT'S HERE! The brand new GUIDE TO MEDICAL PRIVACY AND HIPAA -- a comprehensive, 500-page reference on HIPAA how-to's across every compliance phase, including user-friendly analysis and advice by legal and consulting experts, plus sample forms, checklists, workplans and more -- even regular monthly updates and additions for a year!

Find out more at: <http://www.hipaadvisory.com/wares/HIPAAbook.htm?n>

=====

This week's HIPAAnote...

\*\*\* Minimum Necessary and Role-Based Access \*\*\*

As a covered entity, your organization must make reasonable efforts to limit use of protected health information to the minimum needed to accomplish the intended purpose of the use, disclosure, or request. This requirement does NOT apply to:

- >> Information used or disclosed for treatment
- >> Information given to individuals concerning their own health
- >> Disclosures required by law or for compliance with privacy regulations
- >> De-identified information
- >> Disclosures to another covered entity, if that third party has received authorization by an individual

How will this broad requirement affect you? Your organization must develop and implement policies and procedures that identify the persons or classes of persons who need access to PHI to carry out their job duties. Procedures should also state the categories or types of PHI that is needed to accomplish the job functions, and the conditions under which it is appropriate to access the information. For routine, recurring needs for PHI, you may install standard protocols - but for non-routine needs, a process must be established for review on a case by case basis.

Many health care providers use role-based access to enforce the minimum necessary requirement within automated computer systems. As explained in detail within the proposed Security Rule, the role-based access approach enables organizations to assign one or more defined roles to individuals, based on the information needed to perform that role.

Currently, managers often can approve access to most systems for employees within their departments. Unfortunately, from a privacy perspective, users are often granted access that they never use or need. This could be described, at best, as the maximum necessary to perform their job.

Consider how your organization assigns access to computer systems containing PHI, and ask yourself the following questions: When one user within a defined role needs extra functionality, does everyone with that role get the new functionality? Should they? When a new user is added to the system, do you simply copy the access given to a similar user without determining the minimum necessary? Is there documentation on the level and type of access each role should have? How do your currently authorized access levels compare with Privacy Rule mandates?

Once you have answered these questions, the scalability offered by HIPAA will enable your organization to select the best approach for your environment - as long as the "minimum necessary" standards are met. Then, make sure when your work is done, that you document how minimum necessary determinations are made and how electronic access is assigned, whether it's on an individual basis or to groups of employees. Also, don't forget that even though the Security Rule is not final, covered entities are expected to incorporate security measures to support their new "minimum necessary" policy, procedures and processes.

William M. Miaoulis, Principal  
Phoenix Health Systems

That's today's HIPAAnote...now, pass it along!

=====

Bring your HIPAA questions and ideas to life at... HIPAAlive!

Join nearly 5,000 other thinkers, planners, learners and lurkers who are already members of our sister email discussion list. We almost make HIPAA fun! Almost. (Also available in a PREMIUM version of easy-to-navigate, individually formatted, "cleaned up" digests.)

Subscribe Now! Go to <http://www.HIPAAAdvisory.com/live>

=====

HIPAAnotes are published weekly as a learning tool to help you and your associates stay tuned-in to HIPAA and its implications. Forward it to anyone with a "need to know" through your own internal mailing list, intranet or newsletter -- whatever works for you...

Our HIPAAcratic oath: We'll use your ideas for HIPAAnotes -- send them!  
Email D'Arcy Gue, Editor: [info@phoenixhealth.com](mailto:info@phoenixhealth.com)

=====

You are currently subscribed to hipanotes as: [kmckinst@dmhhq.state.ca.us](mailto:kmckinst@dmhhq.state.ca.us)

To change your list settings or UNSUBSCRIBE, go to:  
<http://www.hipaadvisory.com/signup/change.cfm>

List archives:  
<http://www.hipaadvisory.com/notes/archives.htm>

=====

=